Xollam, the Latest Face of TargetCompany

trendmicro.com/en_us/research/23/f/xollam-the-latest-face-of-targetcompany.html

June 6, 2023

Ransomware

This blog talks about the latest TargetCompany ransomware variant, Xollam, and the new initial access technique it uses. We also investigate previous variants' behaviors and the ransomware family's extortion scheme.

By: Earle Maui Earnshaw, Nathaniel Morales, Katherine Casona, Don Ovid Ladores June 06, 2023 Read time: (words)

After first being detected in June 2021, the TargetCompany ransomware family underwent several name changes that signified major updates in the ransomware family, such as modifications in encryption algorithm and different decryptor characteristics.

The earliest samples of the TargetCompany ransomware appended victims' files with the extension ".tohnichi," the name of its victim enterprise at that time, signifying a targeted attack on the organization of the same name. As a result, it was initially known as the Tohnichi ransomware.

Later, the group continued appending encrypted files with names based on its victims, such as ".artis" for the Artis Zoo in Amsterdam. Other extensions include ".herrco," ".brg," and ".carone."

Industry experts then later identified the ransomware as TargetCompany from the pattern it adopted of appending encrypted files after the company it was targeting.

The variants Tohnichi (active in 2021), Mallox, and Fargo (both active in 2022) targeted vulnerabilities in Microsoft SQL (MS SQL) Server for initial access. We elaborate on the behavior of these variants in our Ransomware Spotlight: TargetCompany.

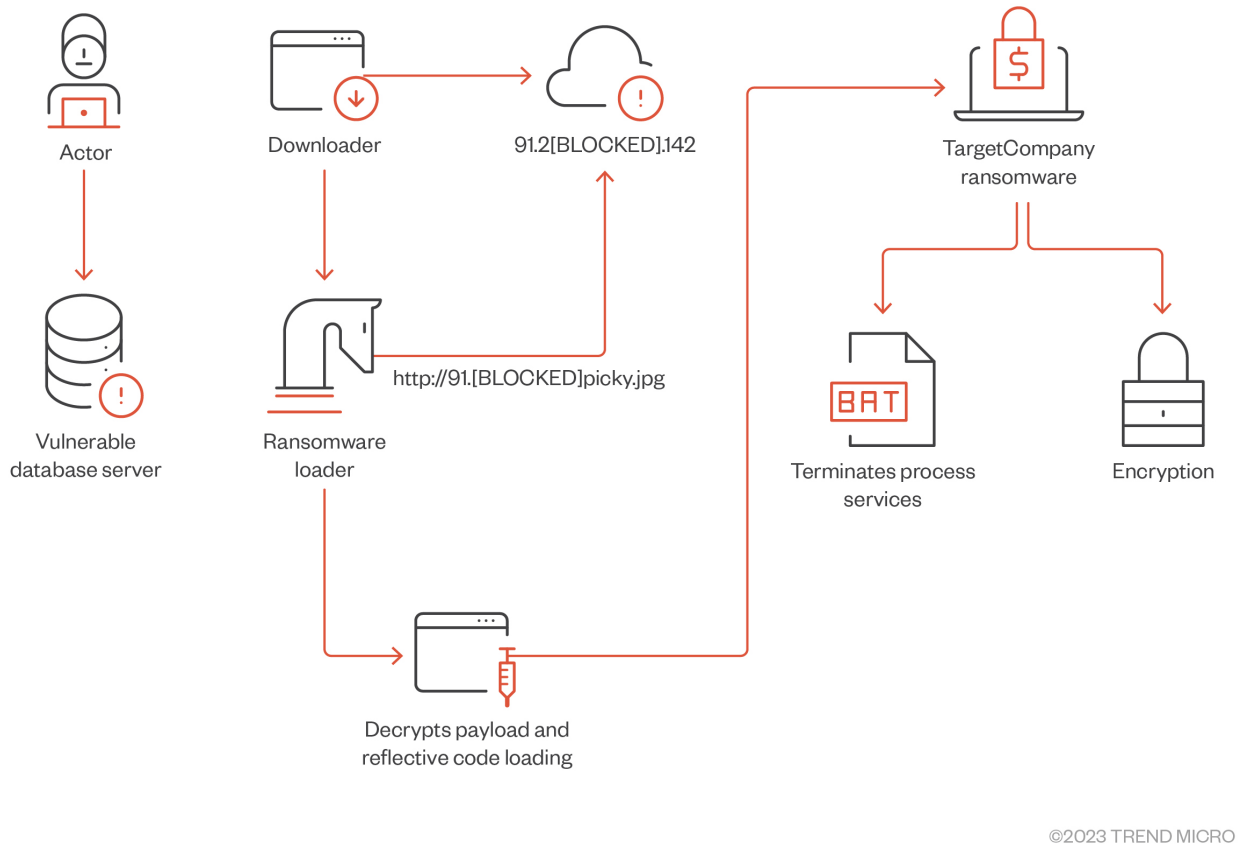

Figure 1. The infection chain of the earlier TargetCompany variants

Our investigations show that its latest variant, Xollam, now deviates from the gang's tried-and-tested initial access method. In this blog, we discuss this latest development in the TargetCompany ransomware's behavior and look into its previous infection chains.

Simultaneously active: Xollam and Mallox variants

In 2023, Xollam was observed as following a technique similar to the one followed by phishing campaigns: using Microsoft OneNote files as initial access to spread and deliver malware. This latest TargetCompany variant executed a spam campaign with malicious OneNote file attachments, a deviation from its roots of targeting vulnerable MS SQL databases.

Based on our investigations, Xollam uses a pseudo-fileless technique through PowerShell, which executes reflective loading to download its payload.

As we discuss in later sections, we have also observed this technique in earlier variants of the TargetCompany ransomware.

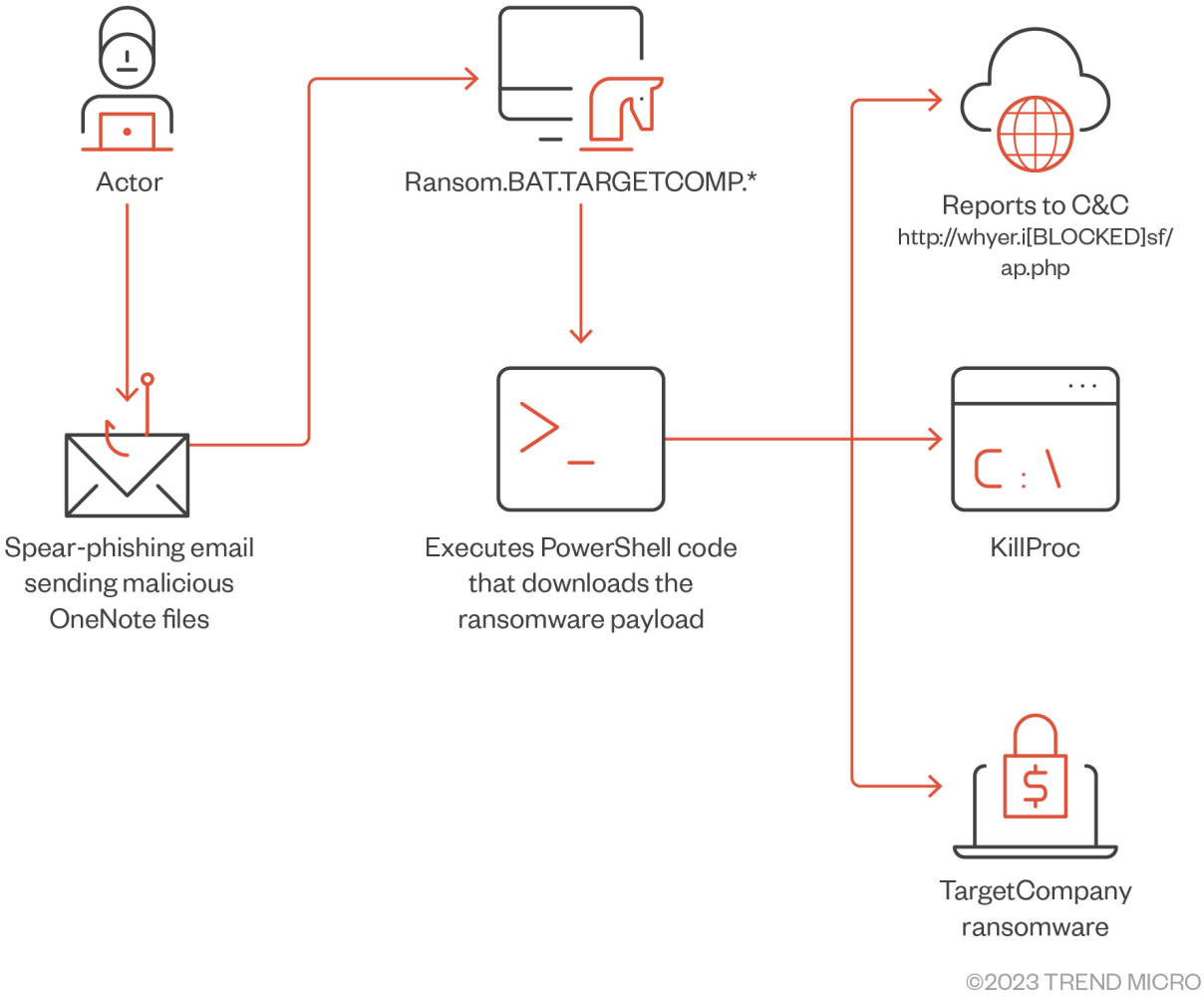

Figure 2. The attack flow of the latest TargetCompany variant, Xollam, which uses malicious OneNote files for initial access

The latest variant of the ransomware, Xollam, was detected in February this year.

In the same month, the older Mallox variant was also active, as it claimed the attack on the Federation of Indian Chambers of Commerce and Industry (FICCI). The gang released 1.28 GB of compressed datasets that included financial balance sheets, employee reimbursement details, bank statements and internet banking credentials, industry audit reports, and documents related to FICCI subcommittees.

Reflective loading, Mallox, and Fargo variants

The Mallox variant of the ransomware was first detected in the wild in October 2021. Later samples in January of the following year showed that the ransomware group started to employ reflective loading as part of its defense evasion.

The Mallox variant connects to an IP address to load the encrypted ransomware, with its download URL only available for approximately 24 hours. Notably, this made the dynamic analysis of old samples difficult.

Our investigations revealed that the payload downloaded by the PowerShell script was a .NET downloader, which would subsequently retrieve an encrypted payload from the command-and-control (C&C) server.

The downloaded file has a random file name and might have different extensions such as ".png," ".bmp," and ".jpg," among others.

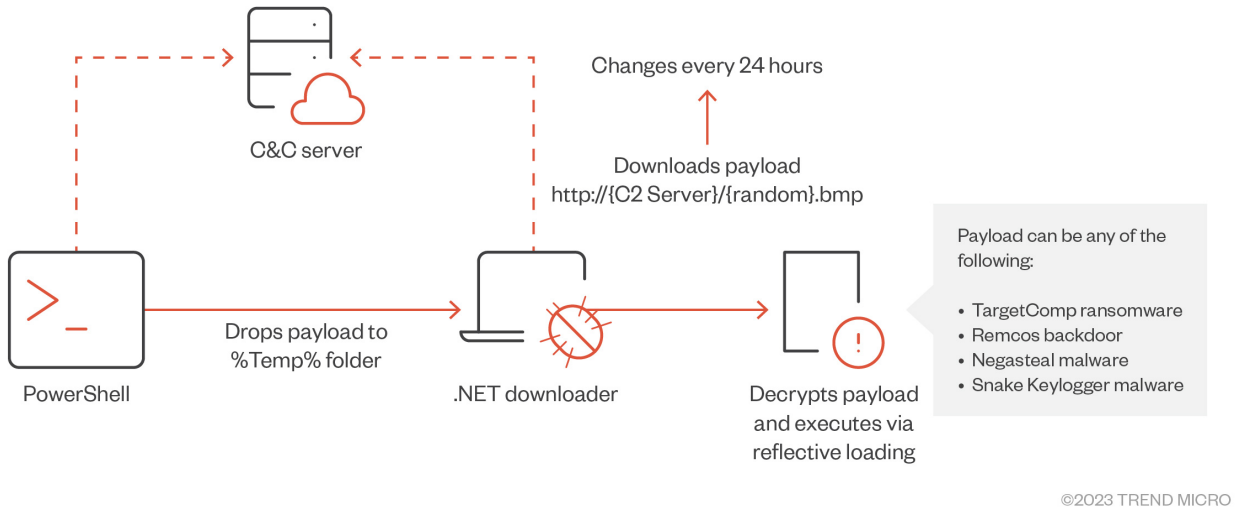

Figure 3. A closer look at the reflective loading technique that TargetCompany threat actors incorporated; the IP address it connects to changes every 24 hours and deploys different payloads

The payload would then be decrypted through XOR or inversion and executed in memory. The specific payload that is downloaded varies depending on the link on the .NET downloader.

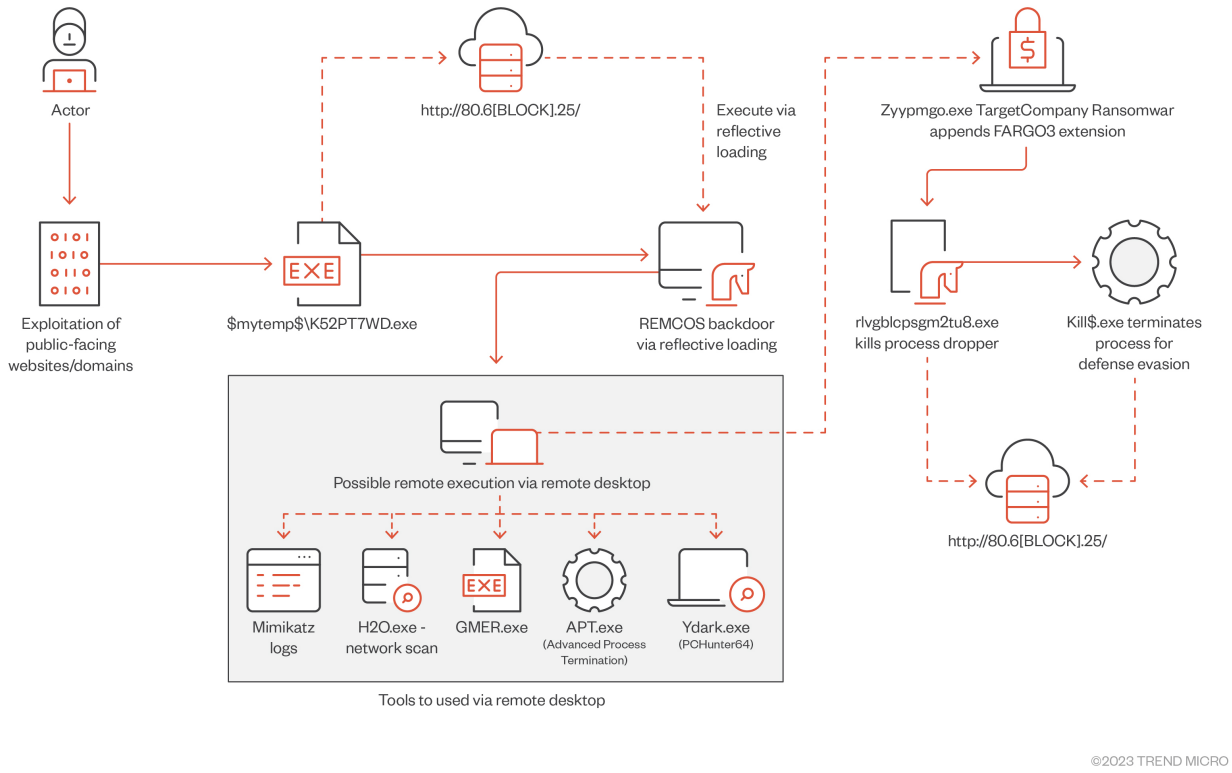

Figure 4. Both Mallox and Fargo variants use a set of tools via remote desktop for defense evasion.

It's important to note that reflective loading enabled the Mallox variant to evade traditional antivirus solutions, making it challenging for organizations to protect themselves against these attacks.

Meanwhile, the Remcos backdoor payload is executed via *WmiPrvSE.exe,* and the payload most likely arrives by exploiting public-facing websites and domains.

Our investigations showed that the gang used different sets of defense evasion and reconnaissance tools such as GMER and Advance Process Termination to manually uninstall antivirus products on the target system. We also observed the presence of *YDArk.exe* (PCHunter64) for performing rootkit behaviors, and that TargetCompany attempts to terminate security-related processes and services by dropping KILLAV.

In addition, the ransomware drops a batch file named *killer.bat* that terminates various services and applications, including GPS-related services. Afterward, it proceeds to steal system information like machine details and other relevant data.

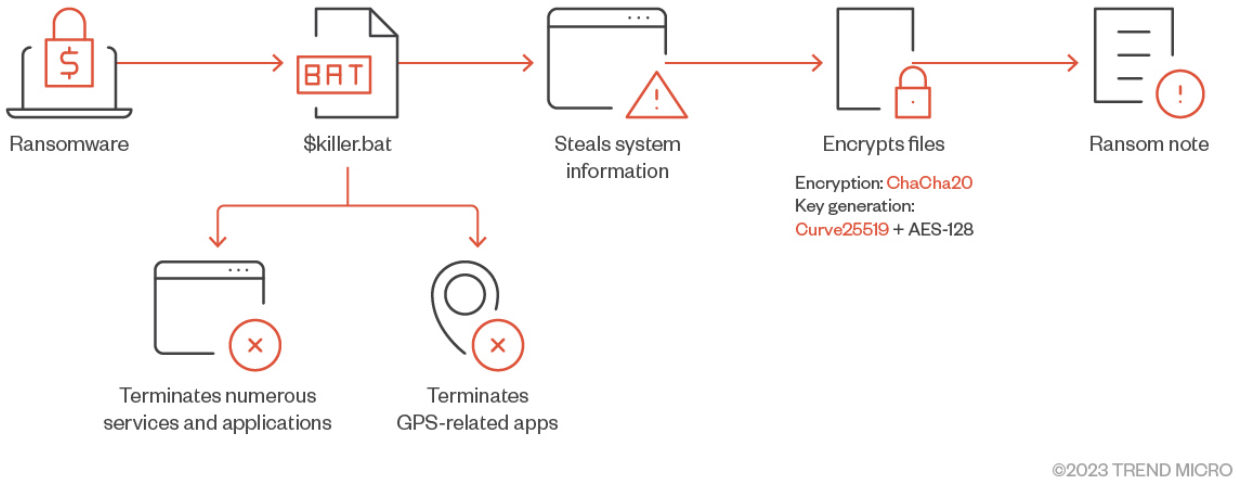

Figure 5. TargetCompany ransomware defense evasion routine

The ransomware encrypts the victim's files using the ChaCha20 encryption algorithm and generates the encryption keys using a combination of Curve25519, an example of elliptic curve cryptography, and AES-128.

In June 2022, the gang targeted other victims with encrypted files appended with the extension ".fargo." We also observed that like Mallox, the Fargo variant employed reflective loading.

In the last two months of 2022, there was an increase in attacks launched by the TargetCompany ransomware using its Mallox variant.

Extortion

While the Mallox and Fargo variants were operating simultaneously in 2022, TargetCompany initiated its double-extortion scheme by setting up a Telegram channel where it could publish stolen information.

In August 2022, just two months after the group launched its Fargo variant, Mallox created a Twitter account where it could announce its victims. Since this account was eventually suspended, the threat actors created a new one.

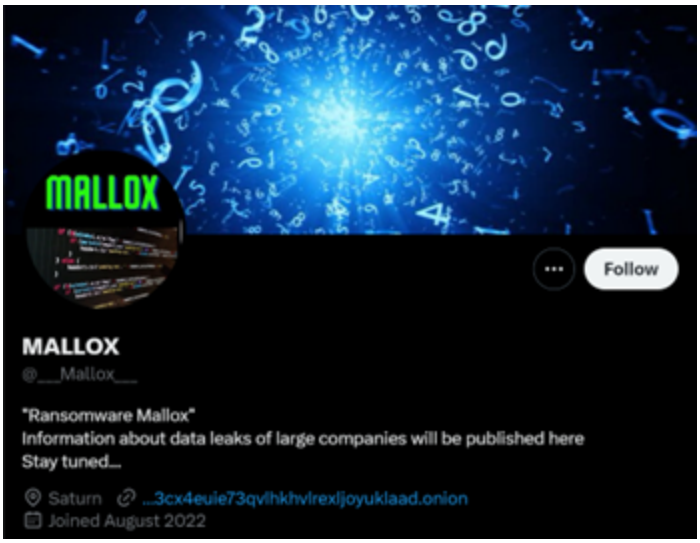

Figure 6. The first Twitter account (eventually suspended) that Mallox created for announcing its victims (top), and the new Twitter account that replaced it (bottom); the new account remains active as of this writing

In November of the same year, Mallox launched its data leak site where, as of writing, it has declared only 20 victims. However, our telemetry data revealed far more attacks at 269 attempts on Trend Micro customers from March 2022 to April 2023.

In a January 2023 interview, threat actors behind TargetCompany said that they choose only a small percentage of their victims to publish on their leak site. They also limit the amount of leaked data to what they deem particularly interesting and claim to have no intention of publishing everything.

While the group said that it remains small and closed, the actors behind it mentioned that they are “open to suggestions.” Interestingly, a new member of the cybercrime forum RAMP under the name “Mallx” was observed recruiting affiliates for the Mallox ransomware-as-a-service (RaaS) affiliate program.

Our investigations also revealed that the ransomware might have connections with other groups such as the BlueSky ransomware, as well as the threat actors who perform brute-force attacks on MS SQL Servers. TargetCompany shares similarities with these groups in terms of threat actor profiles, targets, deployed remote control, and encryption algorithm. We discuss other possible affiliations, as well as victim profiles and behaviors in our Spotlight feature on the ransomware group.

Conclusion

The TargetCompany ransomware is making bolder ventures beyond its tried-and-tested techniques by joining the bandwagon of OneNote phishing campaigns, which allows it to cast a wider net for increased profitability. Within just two years of activity, the threat actors behind

the ransomware are proving their hunger for prolificacy, expanding their business model with a RaaS affiliate program and maintaining several platforms to announce victims and expose stolen data.

We can expect TargetCompany to make even bigger moves in the future, especially since the threat actors behind it have admitted that they created TargetCompany to move away from the restrictions and inflexibility of their previous groups. Now unhindered, the gang will naturally try to maximize profits from its victims.

To protect systems from ransomware attacks, we recommend that both individual users and organizations implement best practices such as applying data protection and backup and recovery measures to secure data from possible encryption or erasure. Conducting regular vulnerability assessments and patching systems in a timely manner can also minimize the damage dealt by ransomware families that abuse exploits.

We advise users and organizations to update their systems with the latest patches and apply multilayered defense mechanisms. End users and enterprises alike can mitigate the risk of infection from new threats like the TargetCompany ransomware by following these security best practices:

- Enable multifactor authentication (MFA) to prevent attackers from performing lateral movement inside a network.
- Adhere to the 3-2-1 rule when backing up important files. This involves creating three backup copies on two different file formats, with one of the copies stored in a separate location.
- Patch and update systems regularly. It's important to keep operating systems and applications up to date and maintain patch management protocols that can deter malicious actors from exploiting any software vulnerabilities.